

#6
KWS
415-03**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

| | |
|------------------------|-------------------------------------|
| Applicant and Inventor | Ho Keung, TSE. |
| Filing Date | 12/01/95 |
| Application Number | 08/587,448 |
| Group Art Unit | 2132 |
| Examiner | Gilberto Barron Jr. |
| H.K. Tel & FAX | (852) 8105, 1090 & (852) 8105, 1091 |
| Email | t9224@netscape.net |

Official
4/11/03

Hon. Commissioner of Patents and Trademarks, Washington, D.C. 20231, Box AF.

Sir,

Appeal Brief

(1) **Real party in interest--** As I am the sole inventor and applicant, there is no other real party in interest other than me.

(2) **Related appeals and interferences—** another US patent application 09/112,276 of mine for the same invention as the present application (therefore, both applications are now under a provisional double patenting rejection) is under appeal.

Further, pls note that the claims 1, 12 of the present application 08/587,448 is equivalent to the claims 1, 21 as amended in "Substitute Amendment (submitted with Substitute Appeal Brief" which is to be submitted with Substitute Appeal Brief of the another US patent application 09/112,276 to the Board. And therefore, should claims 1, 12 of the present application 08/587,448 be decided as allowable, then the amendment of claims 1, 21 as proposed in "Substitute Amendment (submitted with Substitute Appeal Brief" of the another US patent application 09/112,276 should be entered and allowed.

(3) **Status of Claims :**

20 claims presented, namely as, claims 1-7, 9-21.

Claims 2-7, 9-11, 13-21 are withdrawn from Appeal.

Claims 1, 12 remains and both are independent.

(4) Status of Amendments :

Amendment on claims 1,12, entitled "Formal Response to First Office Action", responsive to the non-final office action for re-opening prosecution— entered.

Amendment entitled "Amendment on Description & Claim 17" dated : Dec 3, 2002— not entered.

(5) Summary of Invention :

The following is a concise explanation of the invention defined in the independent claims 1, 12 :

Claim 1 recites a method(refer to description, P.8 first paragraph of item 5)

for protecting software from unauthorised use, comprising the steps of :

determining the existence of an identity software (corresponding to "EI sub-program", refer to description, P.4 item 2) in association with a processing means under control of a user ;

using a favourable result of said determination of existence as a pre-condition for providing said user access to said software desired to be protected on said processing means ;

wherein said identity software being for enabling electronic money transfer operation(s) for which a rightful user of said software desired to be protected has to be responsible ;

wherein access to said software desired to be protected is being provided without causing a said operation being performed .

Claim 21 recites a method (refer to description, P.7 whole page to P.8 first paragraph)

for verifying identity of a user of a data processing apparatus, comprising the steps of:

receiving, by said data processing apparatus (corresponding to "IBM PC", refer to description, P.3, under the heading "Detailed description of the preferred embodiments", line 3), information (corresponding to "EI sub-program", refer to description, P.4 item 2) specific to a user and necessary for accessing an account of said user;

verifying said account being valid (refer to description, P.7 first paragraph), by an electronic transaction system, by use of said information received by said data processing apparatus;

using by said data processing apparatus, said account validity being verified as a pre-condition for providing user access to at least a part of the functionality of said data processing apparatus;

wherein said method is being performed without charging said account and said at least a part of functionality being not related to said validity status of said account.

(6) Issues :

- A) Whether "unencrypted identity", in description, P.7, first paragraph, line 4 is a typographical error and should be "encrypted identity" ?
- B) Whether claims 1 and 12 are unpatentable under 35 U.S.C. 112, second paragraph, as failing to set forth the subject matter which applicant(s) regard as invention, as readable on the Final Office Action, P.3, section 5 ?
- C) Whether claims 1 and 12 are unpatentable under 35 U.S.C. 103(a) over Wiedemer(4,796,181) in view of Haas et al (5,719,938 issued Feb 17, 1998, filing date Aug 1, 1994), as readable on the Final Office action, P.4 , section 6 ?

(7) Grouping of Claims

Regarding rejection of claims 1 and 12 under 35 U.S.C. 103(a) over Wiedemer(4,796,181) in view of Haas et al, as readable on the Final Office action, P.4 , section 6, claims 1 and 12 do not stand or fall together.

(8) Argument**Argument A:**

Whether "unencrypted identity", in description, P.7, first paragraph, line 4, is a typographical error and should be "encrypted identity" ?

As readable in the description, P.7, first paragraph, lines 3-5 that "In the initialization process, the central program sends to the central computer, as mentioned herein above in item 2, an unencrypted identity of the user", the term "unencrypted" is a typographical error and the correct term should be "encrypted", for the reason that in P.4, item 2 of the description, it is disclosed a "Sub-program for providing an Encrypted Identity (EI sub-program)", in which unencrypted identity or its equivalent is not being mentioned.

The Board is respectfully requested to indicate acceptance of this argument so that I can file a formal request or correcting this typographical error thereafter.

Argument B:

Whether claims 1 and 12 are unpatentable under 35 U.S.C. 112, second paragraph, as failing to set forth the subject matter which applicant(s) regard as invention, as readable on the Final Office Action, P.3, section 5 ?

In this rejection, the Examiner rejects all the claims including claims 1, 12.

The Examiner's reasons of this rejection such as "The claims of this application continue to be indefinite. Applicants chose of alternative expressions and narrative dialog impede the formation of a claim that positively set forth the element that comprises Applicant's invention ..." should only be applicable to the claims when prosecution is reopened. It should not be applicable to claims 1, 12, after amendment on claims 1,12, entitled "Formal Response to First Office Action" which being responsive to the non-final office action for re-opening prosecution, is entered .

Argument C:

Whether claims 1 and 12 are unpatentable under 35 U.S.C. 103(a) over Wiedemer (4,796,181) in view of Haas et al (5,719,938 issued Feb 17, 1998, filing date Aug 1, 1994), as readable on the Final Office action, P.4 , section 6 ?

Examiner's Argument

As the Examiner has admitted in the Final Office action, P.4, section 6, second paragraph, in his arguments in support of 103 rejection of claims 1 and 12, "The Wiedemer patent provides for an identity means to determine authorization if a user and provides for information that leads to a billing charge, but does not disclose the step of not causing an operation for which an authorized user is responsible for".

But the Examiner further stated, in the Final Office action, P.4, section 6, third paragraph, "The patent to Haas et al teaches a method for providing secure access to shared information such as a newspaper, see column 1, lines 20-35. The Haas patent teaches deterrents for discouraging users from providing useful information to others to access the information in question. Column 5, lines 47-54 teach a first deterrent as causing a rightful user's credit card number to display to discourage a rightful user from sharing the information to access the secured information to others".

Finally the Examiner concluded in the fourth paragraph, "it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Wiedemer method as taught in Hass by causing a rightful user's credit card number to be displayed in order to discourage rightful user's from sharing information with others who are not the rightful user(s).

The Examiner also states that, in the Final Office action, P.2, section 3, "it is the claims that are to distinguish from the prior art and not that the prior art operates differently".

Comments on Patentability of Claim 1

The Examiner incorrectly applies Haas et al's deterrent to Wiedemer, for the following reasons:

- 1) It is respectfully submitted that, Wiedemer's billing system's most important purpose is to monitor usage of a software so as to charge a user based on amount of usage of the same software (refer to abstract), therefore if its purpose is to be changed to charge the user in the form of regular subscription (refer to Haas et al, col., 2, lines 8,9, *"suitable for use in providing secure access electronic newspapers and multimedia documents"*; col., 3, lines 56-59, *"the user i transmits ...his credit card number (for billing purposes)"*; col. 4, lines 45, 46, *"a user's access permission expires"*) or a fixed price for perpetual use(as mentioned in Wiedemer, *"Background of the invention"*, col. 1, lines 19-23) or the like, etc., such that payment is independent of amount of usage, then there would require a substantial reconstruction and redesign of the elements in Wiedemer's billing system as well as a change in the basic principle under which the construction was designed to operate. Therefore, it would not be obvious to one with ordinary skill in the art to modify Wiedemer's billing system to not do the monitor work during the time the protected software is being used and not to charge a user based on amount of usage, so as to meet the important limitation of claim 1 that "access to said software desired to be protected is being provided without causing an electronic money transfer operation being performed".
- 2) Wiedemer's requirement of "monitoring usage of software so as to charge a rightful user based on amount of usage of software", that is billing operation,

is already providing a better effect of discouraging the rightful user from sharing a software with other people, than Haas et al's deterrent. Because if the rightful user allows another person to use the software, he is bound to be charged by Wiedemer's billing system, whereas Haas et al's deterrent although will display the rightful user's credit card information to that person, that person may not make use of the information to make any transaction. Thus, there has no motivation for one with ordinary skill in the art to modify Wiedemer's billing system with Haas et al's deterrent.

- 3) Further, the purpose of Wiedemer's billing operation is to charge a rightful user basing on the amount of usage, and to make money. Therefore, as long as the usage of software can be monitored and the rightful user can be charged, then one with ordinary skill in the art would not prevent other person from using the protected software under the permission of the rightful user, by applying Haas et al's deterrent to Wiedemer. In doing so, the prime purpose of Wiedemer, that is, making money, will be undermined.

If Wiedemer method was to be modified with Haas et al's deterrent, the result would be a method comprising 1) Wiedemer's billing system to monitor usage of software so as to charge a user based on amount of usage of software; as well as 2) Haas et al's deterrent which causes a rightful user's credit card number to be displayed in order to discourage rightful user's from sharing information with others. Thus, the above reasons for Wiedemer cannot meet claim 1 is also applicable to the result as far as the part corresponding to Wiedemer's billing system therein is concerned. Similarly, the reasons for Haas et al. failing to meet claim 1 is also applicable to the result as far as the part corresponding to Haas et al's deterrent therein is concerned, as follows :

The present invention as claimed by claim 1 is directed to a method for protecting software from unauthorised use. As readable thereon, it requires existence of an identity software in association with a processing means as a pre-condition for providing user access to the software desired to be protected on the processing means; wherein said identity software being for enabling electronic money transfer operation(s) for which a rightful user of said software desired to be protected has to be responsible.

As seen, claim 1 is directed to a method useful for protecting a software from unauthorised use at a time no payment for the use thereof is required, for reason such as payment is being made at a earlier time.

Further, although not indicated in claim 1, it is obvious that the identity software is stored in a computer device and is not in a human visible form and not accessible to any one else except under the permission of the rightful user.

Haas et al's deterrent although can meet claim 1's requirement of "no electronic money transfer operation for which an authorized user is responsible for, such as actual payment", it has a drawback that the rightful user have to make sure no other people is around before he can use the software.

It is an essential feature in Haas et al.'s deterrent that a rightful user's credit card number has to be displayed, and it is therefore not obvious to one with ordinary skill in the art to modify it by not having the credit card number to be displayed; and further to make use of the electronic transaction capability of the credit card number to create a software to enable a processing means such as a computer to make electronic money transfer operation(s) to meet requirement of "identity software" of claim 1; and still further, requires a favourable result of a determination of existence of such an identity software as a pre-condition for providing user access to the software desired

to be protected, but "without causing an electronic money transfer operation being performed", so as to amount to the present invention as defined by claim 1.

Further, it is respectfully submitted that "the credit card number to be displayed" of Haas et al. deterrent and "credit card number exist in and used by a software to enable electronic money transfer operation(s)" as mentioned above, exist in a computer in 2 technical distinguishable forms. The reason is, the former is in human readable form and, the latter which as mentioned above, is a "identity software" meeting the requirement of claim 1, is in a form agreeable with a common communication protocol for communicate to/understandable by an existing remote transaction system. Thus, "the credit card number to be displayed" of Haas et al. deterrent cannot meet the requirement of "identity software being for enabling electronic money transfer operation(s)" of claim 1.

Further, it is considered that, although "credit card number exist in and used by a software to enable electronic money transfer operation(s) such as internet transactions" is a well known technology, it would not be obvious for one with ordinary skill in the art to use it in place of "displaying a rightful user's credit card number" of Haas et al. deterrent in the manner as taught by claim 1, for the reason that the credit card number contained in such a software is alterable by the rightful user from time to time and may be invalid or incorrect. Further, even if a verification of its validity or correctness has to take place when payment is to be made by means thereof, the rightful user can immediately change it thereafter. Thus, such a software is not capable of being used for software protection in the manner as suggested by the present invention as defined by claim 1.

Accordingly, 103(a) rejection of claim 1 basing on Haas et al. and Wiedemer should be withdrawn and is respectfully requested.

Comments On Patentability of Claim 12

In addition to the above, the Examiner also states that, in the Final Office action, P.2, section 3, claim 12 recites "verifying said account, by an electronic transaction system", this is shown in Haas et al. at column 3 lines 55-60.

The Examiner's rejection is respectfully traversed. Although not readable on claim 12, the present invention as defined by claim 12 is directed to a method for protecting a data processing apparatus from unauthorised use. It is respectfully submitted that, it is an innovative feature of the present invention as defined by independent claim 12 that, verifying identity of a user of a data processing apparatus, I) by receiving information specific to a user and necessary for accessing an account of the user; II) verifying the user account being valid; III) and using the account validity being verified as a pre-condition for providing user access to at least a part of the functionality of the data processing apparatus, without charging the account and that at least a part of functionality being not related to the validity status of said account.

In Haas et al. at column 3 lines 55-60, "the user i transmits ...his credit card number (for billing purposes)". Wiedemer patent similiarly provides for an i dentity means to determine authorization of a user and provides for information that leads to a billing charge.

It is clear that the credit number of Haas et al. at column 3 lines 55-60 as well as Wiedemer's identity means both being for billing purposes cannot meet the important requirement of claim 12, that is "validity of a user account should be checked, without charging the account for providing the user access to a data processing apparatus", as required by claim 12.

As seen, claim 12 is directed to a method useful for protecting a apparatus from unauthorised use at a time no payment for the use thereof is necessary, whereas Wiedemer and Haas et al. (column 3 lines 55-60) are directed to receiving payment from a user in order to provide right of access to information and are therefore should be not relevant to claim 12.

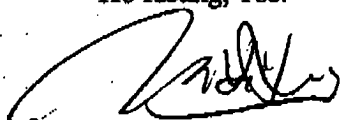
Further, Haas et al. 's deterrent, as readable on column 5, lines 47-54, discloses a software for causing a rightful user's credit card number to be displayed, to discourage a rightful user from sharing another software which being for decrypting a commercial software product, to other people.

This deterrent can only be useful if the credit account concerned is valid, but a verification of the account validity as required by the present invention as defined by claim 12, for the purpose of verification of user identity, without receiving any payment, is neither disclosed or suggested by Haas et al and Wiedemer, whole document. This is a problem inherent in Haas et al's deterrent and not being discovered and overcome until the present invention as defined by claim 12.

Thus, this requirement of claim 12 cannot be met even if Haas et al was to be combined with Wiedemer in any manner.

Accordingly, 103(a) rejection of claim 12 basing on Haas et al. and Wiedemer should be withdrawn and is respectfully requested.

Respectfully submitted,
Applicant & Sole Inventor,
Ho Keung, Tse.



(9) Appendix.

1. A method for protecting software from unauthorised use , comprising the steps of :

 determining the existence of an identity software in association with a processing means under control of a user ;

 using a favourable result of said determination of existence as a pre-condition for providing said user access to said software desired to be protected on said processing means ;

 wherein said identity software being for enabling electronic money transfer operation(s) for which a rightful user of said software desired to be protected has to be responsible ;

 wherein access to said software desired to be protected is being provided without causing a said operation being performed .

12. A method for verifying identity of a user of a data processing apparatus, comprising the steps of :

receiving, by said data processing apparatus, information specific to a user and necessary for accessing an account of said user ;

verifying said account being valid, by an electronic transaction system, by use of said information received by said data processing apparatus;

using by said data processing apparatus, said account validity being verified as a pre-condition for providing user access to at least a part of the functionality of said data processing apparatus ;

wherein said method is being performed without charging said account and said at least a part of functionality being not related to said validity status of said account.